



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER OF PATENTS AND TRADEMARKS  
Washington, D.C. 20231  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/098,204	06/16/1998	HOWARD R. UDELL	200.1099	3784

23280 7590 11/05/2002

DAVIDSON, DAVIDSON & KAPPEL, LLC  
485 SEVENTH AVENUE, 14TH FLOOR  
NEW YORK, NY 10018

EXAMINER

VU, THONG H

ART UNIT PAPER NUMBER

2142

DATE MAILED: 11/05/2002

Please find below and/or attached an Office communication concerning this application or proceeding.



**UNITED STATES PATENT AND TRADEMARK OFFICE**

COMMISSIONER FOR PATENTS  
UNITED STATES PATENT AND TRADEMARK OFFICE  
WASHINGTON, D.C. 20231  
[www.uspto.gov](http://www.uspto.gov)

**BEFORE THE BOARD OF PATENT APPEALS  
AND INTERFERENCES**

Paper No. 25

Application Number: 09/098,204  
Filing Date: June 16, 1998  
Appellant(s): UDELL ET AL.

**MAILED**

NOV 05 2002

Technology Center 2100

---

Morey B. Wildes  
For Appellant

**EXAMINER'S ANSWER**

This is in response to the appeal brief filed 8/12/02.

**(1) *Real Party in Interest***

A statement identifying the real party in interest is contained in the brief.

**(2) *Related Appeals and Interferences***

A statement identifying the related appeals and interferences which will directly affect or be directly affected by or have a bearing on the decision in the pending appeal is contained in the brief.

**(3) *Status of Claims***

The statement of the status of the claims contained in the brief is correct.

**(4) *Status of Amendments After Final***

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

**(5) *Summary of Invention***

The summary of invention contained in the brief is correct.

**(6) *Issues***

The appellant's statement of the issues in the brief is correct.

**(7) *Grouping of Claims***

Appellant's brief includes a statement that claims of the following groups of claims do not stand or fall together and provides reasons as set forth in 37 CFR 1.192(c)(7) and (c)(8).

Group I: claims 1-4 and 44-47

Group II: claims 6-10, 14-15 and 17

Group III: claims 5 and 13

Group IV: claims 18 and 19

**(8) Claims Appealed**

The copy of the appealed claims contained in the Appendix to the brief is correct.

**(9) Prior Art of Record**

Hansen, Enhancing Documents with Embedded Programs: How Ness Extends Insets in the Andrew Toolkit, IEEE 1990

5903723	Beck et al	5-1999
6006328	Drake	12-1999
5787247	Norin et al	7-1998

**(10) Grounds of Rejection**

The following ground(s) of rejection are applicable to the appealed claims:

1 Claims 1-10,13-15,17-47 are rejected under 35 U.S.C. § 103 as being unpatentable over Hansen [Enhancing documents with embedded programs: How Ness extends insets in the Andrew Toolkit] in view of Beck et al [Beck 5,903,723]

2 As per claim 1, Hansen discloses a method for creating a self-destructing document, comprising the steps of creating an executable module which instructs a computer to automatically delete the document to which the executable module is attached when the document, based on a preselected expiration date is expired; attaching the executable module to the document [Hansen, page 28 col 2 lines 4-13]

However Hansen fails to detail the a preselected expiration date is expired. Beck discloses a Email message with attachment automatically deleted by a time limit and

encryption and decryption keys [Beck col 7 lines 1-18]. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the technique of a email message automatically deleted by an expiration date as taught by Beck and Hansen's system. By doing so it would improve the security and reliability for message storage and transaction between client/server.

3 As per claims 2-4, Hansen-Beck disclose the executable module is an executable code, program, macro as inherent feature of software code [Hansen page 28 col 2 lines 4-13]

4 As per claim 5, Hansen-Beck disclose the step of executing the executable module when the document is opened [Hansen page 28 col 2 lines 4-13]

5 Claims 6-10,13-15,17-47 contain the same limitations that were addressed in rejecting claims 1-5 above. Examiner would take an Official Notice, that the technique self-destruction of data, message, software will be activated whenever user attempt to access an unauthorized feature is well-known in the network security art [see Shear, Thorne references]. By the same rationale applied above, claims 6-10,13-15,17-47 are rejected.

6 Claims 1-10,13-15,17-47 are rejected under 35 U.S.C. § 103 as being obvious over Drake [6,006,328] in view of Norin et al [Beck 5,787,247]

7 As per claim 1, Drake discloses a method for creating a self-destructing document, comprising the steps of creating an executable module which instructs a

computer to automatically delete the document to which the executable module is attached when the document, based on a preselected expiration date is expired; attaching the executable module to the document [such as a message with a header is attached by a executable code or software which is designed to self-destruct, Drake Fig 10, col 7 lines 43-52]

However Drake fails to detail the a preselected expiration date is expired. Norin discloses a Email message with time-based expiration date wherein an object is older a set time will be deleted automatically [Norin col 24 lines 1-25]. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the technique of a email message automatically delete by an expiration date as taught by Norin and Drake's system. By doing so it would improve the reliability for data storage and transaction between client/server.

8 As per claims 2-4, Drake-Norin disclose the executable module is an executable code, program, macro as inherent feature of software code [Drake Fig 10, col 7 lines 43-52]

9 As per claim 5, Drake-Norin disclose the step of executing the executable module when the document is opened [Drake Fig 10, col 7 lines 43-52]

10 Claims 6-10,13-15,17-47 contain the same limitations that were addressed in rejecting claims 1-5 above. Examiner would take an Official Notice, that the technique self-destruction of data, message, software will be activated whenever user attempt to access an unauthorized feature is well-known in the network security art [see Shear,

Thorne references]. By the same rationale applied above, claims 6-10,13-15,17-47 are rejected.

**(11) Response to Argument**

**Rejection Based Upon the Hansen-Beck Combination:**

Group I: Claims 1-4 and 44-47

1. Appellant argues Hansen does not disclose a method for creating a self-destructing document.

As to group I, Hansen teaches enhanced documents with embedded scripts that have capability of automatically performing functions such as delete a file. Hansen also teaches hypertext document can be created easily as enhanced document which applied to the multimedia mail community such as a Hypercard with an embedded object forms wherein the set of trigger events are defined and one of embedded script in document could trigger a delete file function. It is well-known in the art that a delete file function could be deleted a specific document which defined by user or itself as claimed by appellant [Hansen pages 23-29,30,32].

Group II : Claims 6-10,14,15 and 17

2. A. Appellant argues the prior art does not teach email messaging system.

As to point A, Hansen teaches an embedded script in document designed to delete a file such as Hypertext document or multimedia mail [Hansen pages 23,29]. It is obvious to one of the ordinary skill in the Data processing art that an email message contains a delete file function could automatically self-destruct (i.e.: event trigger) or delete other file by design.

3. B. Appellant argues the prior art does not teach delete a file when a predetermined condition is selected.

As to point B, Examiner notes Becker discloses an email with attachment message may be automatically deleted after a given time limit, such as 90 days (i.e.: expiration date) [Beck col 7 lines 1-17]. It is obvious the predetermined condition to delete the email message with attachment could be changed by the time limited, the option of email function (i.e.: saved by one or several day, week, month) as a variable subject matter.

Group III: Claims 5 and 13.

4. Appellant argues the prior art does not teach the executable module executes when the document or email message to which the module attached is opened.

Examiner notes the prior art taught the Hypertext document (i.e.: a multimedia email, a Hypercard) when opened could trigger an event such as a birthday song or other function (i.e.: delete a file) [Hansen pages 23-24, 28-32]

Group IV: Claims 18 and 19.

5. Appellant argues the prior art does not teach encryption of a document or email that is attached to an executable module.

Examiner notes the prior taught the email message with encryption and decryption key [Beck col 7 lines 19-40]. It is obvious the option using encryption of a document or email as an option which was well-known in the art.

C. No Prima Facie Rejection Made Based on Hansen and Beck:

6. Appellant argues there is no suggestion to combine Hansen and Becker.



Examiner notes both prior art taught the transaction electronic message between client and server. Hansen taught a multimedia mail environment including a Hypercard which embedded or attach a script with a set of event trigger when activated would perform a predefined function (i.e.: birthday song, delete file). Beck taught an email message environment including the encryption feature. Therefore it is obvious to the one of ordinary skilled in the art to combine the encryption email technique as taught by Becker into the Hansen's apparatus in order to utilize the multimedia mail in order to improve the security and protection the email message with embedded script . Doing so would provide the more security and reliability for storage and transaction of the electronic messages in network environment.

Rejection Based Upon the Drake-Norin Combination:

Group I: Claims 1-4 and 44-47

7. Appellant argues the prior art does not teach a method of self-destructing document.

Examiner notes the prior art taught email message contained a self executable code such as viruses which destroy itself or other documents [Drake abstract].

Group II: Claims 6-10,14,15 and 17.

8. Appellant argues the prior art does not teach an email system that is configured to create the message, transmit the message and attach the executable module to the message.

Examiner notes the prior art taught email system with an expiry date, encryption key, viewing the executable program such as software designed to self-destruct [Drake col 7 lines 43-52] or viruses [Drake col 1 line 55-col 2 line 50] which is embedded or attach to the email message as a well-known feature.

Group III: Claims 5 and 13.

9. Appellant argues the prior art does not teach create and activate the self-destructing document.

Examiner notes the prior art taught email system with software designed to self-destruct [Drake col 7 lines 43-52] or viruses [Drake col 1 line 55-col 2 line 50]. It is well-known in the art that the viruses as an executable code self-activate and destruct document.

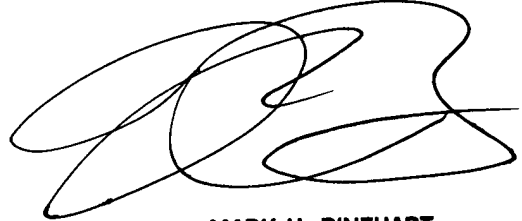
Group IV: Claims 18 and 19.

10. Appellant argues the prior art does not teach the email message is encrypted.

Examiner notes the email message with encrypted technique [Drake Fig 11, col 3 lines 45-50, col 4 lines 50, col 5 line 63-col 6 line 3, col 8 lines 39-53].

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,



MARK H. RINEHART  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100

THONG VU



November 4, 2002

Conferees



ROBERT B. HARRELL  
PRIMARY EXAMINER

DAVIDSON, DAVIDSON & KAPPEL, LLC  
485 SEVENTH AVENUE, 14TH FLOOR  
NEW YORK, NY 10018